

Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 12 October 2004 Meeting

GSA; 1800 F Street; Room 5141B; Washington, DC

A. AGENDA

- 1) Welcome & Opening Remarks / Introductions
- 2) Discussion of Minutes from 14 September 2004
- 3) Status of Email Votes Since Last FPKIPA Meeting
- 4) Discussion Topic #1: FBCA CP Requirement for US Citizenship
- 5) Discussion Topic #2: Signing Procedures for Email Votes
- 6) Discussion Topic #3: Facilitating Compliance with Annual Audit Requirements
- 7) Federal Identity Credentialing Committee (FICC) Report
- 8) FPKI Certificate Policy Working Group (CPWG) Report
- 9) Federal PKI Architecture Operational Authority (FPKIA OA) Report
- 10) Other Topics
- 11) Meeting Adjourned / Next Meeting Plans

B. ATTENDANCE LIST

VOTING MEMBERS

Organization	Name	Email	Telephone
Dept of Commerce (NIST)	Polk, Tim	tim.polk@nist.gov	301.975.3348
Dept of Defense	Hanko, Dave	djhanko@missi.ncsc.mil	410.854.4900
Dept of Energy	Breland, Mary Ann	maryann.breland@hq.doe.gov	301.903.7245
Dept of Justice	Woods, Janice	janice.woods@usdoj.gov	202.616.9211
Dept of State	ABSENT		
Dept of the Treasury	ABSENT		
GSA	Temoshok, David	david.temoshok@gsa.gov	202.208.7655
NASA	DeYoung, Tice	tdeyoung@hq.nasa.gov	202.358.2145
OMB	ABSENT		
USDA/NFC	ABSENT		

OBSERVERS

Organization	Name	Email	Telephone
ACES	Duncan, Steve	stephen.duncan@gsa.gov	202.708.7626
Dept of Defense	Mitchell, Debbie	dmmitt3@missi.ncsc.mil	410.854.4900
Dept of State	Froehlich, Charles	froehlichcr@state.gov	202.203.5069
Dept of the Treasury (eValid8)	Dilley, Brian	brian.dilley@evalid8corp.com	443.250.7681
FICC	Petrick, Brant	brant.petrick@gsa.gov	202.208.4673
FPKIA OA (Mitretek)	Stern, Michael	michael.stern@mitretek.org	703.610.1530
FPKIA OA Director (GSA)	Jenkins, Cheryl	cheryl.jenkins@gsa.gov	571.259.9923
FPKIPA Secretary (IATAC)	Lentz, Mark	lentz_mark@bah.com	410.684.6520
GSA	Cornell, John	john.cornell@gsa.gov	202.501.1598
HHS	Alterman, Peter	altermap@mail.nih.gov	301.252.8846

C. MEETING ACTIVITY

Agenda Items 1 & 2

Introductions / Vote on Approval of Meeting Minutes

Mr. Tim Polk, NIST and FPKIPA Co-Chair, called the meeting to order at 9:40 a.m. with attendee introductions.

Regarding the 14 September 2004 FPKIPA meeting minutes, they were not completed prior to this meeting, so they will be distributed to the FPKIPA via email at a later date for review and email vote.

Agenda Item 3

Status of Email Votes Since Last FPKIPA Meeting

There were three email votes conducted since the last FPKIPA meeting on 14 September 2004 and the tabulated email vote records were distributed via email prior to the meeting (see Appendix A).

The three items voted on via email and their results were:

- 1) FBCA CP Change Proposal 2004-02 (Vote Request – 09/21/04 / **Approved by a vote of 10 Yes votes out of 10 voting members – 09/24/04**)
- 2) E-Governance CA Certificate Policy Change Proposal 2004-02 (Vote Request – 09/21/04 / **Approved by a vote of 10 Yes votes out of 10 voting members – 09/24/04**)
- 3) Federal Common Policy Framework CA (Vote Request – 10/8/04 / **Approved by a vote of 9 Yes votes and 1 non-cast votes out of 10 voting members – 10/08/04**)

Agenda Item 4

Discussion Topic #1: FBCA CP Requirement for US Citizenship

Some observations that were shared at the beginning of the discussion:

- There are no established metrics that organizations use for measuring loyalty, trustworthiness, and integrity.
- The Pharmaceutical Bridge may be setting up CAs in France, Germany, and the UK.
- Foreign nationals are employed at HEBCA and other places.

Since the 14 September FPKIPA meeting, Judy Spencer was able to discuss this issue with Mr. Gil Nolte, DoD PKI PMO Director. Although no exact FBCA CP text changes were discussed, the following conclusions can be asserted from his current thinking on this issue. Of course, DoD will have an opportunity to review and make a final decision on any FBCA CP Change Proposals that address this subject.

- DOD was open to discussion on the US citizenship issue.
- If “U.S. person” becomes part of the FBCA CP, it may require security clearances.
- U.S. citizenship doesn’t guarantee a person’s loyalty, trustworthiness, and integrity.
- PKIs need to employ residents/citizens of the country where it resides, for High assurance, at a minimum.
- The Fed PKI, at all assurance levels (including the SSPs for FICC, should still be required to have U.S. citizens personnel in Trusted Role positions.
- DoD is concerned about role definitions and requirements for background checks being maintained.

The white paper on this subject will be updated to facilitate further progress on this issue. The FPKIPA voting members were asked to send existing definitions from any of their organizations' policy documentation or procedures/metrics for measuring "loyalty, trustworthiness, and integrity" to Dr. Peter Alterman, HHS, by 20 October 2004.

ACTION (093): The FPKIPA voting members are to send existing definitions from any of their organizations' policy documentation or procedures/metrics for measuring "loyalty, trustworthiness, and integrity" to Dr. Peter Alterman, HHS, by 20 October 2004.

Agenda Item 5

Discussion Topic #2: Signing Procedures for Email Votes

Background

Dr. Tice DeYoung, NASA, had asked in a previous FPKIPA meeting that the FPKIPA voting members use either "\S\" or "Signed" in addition to their name at the bottom of their email when casting official FPKIPA votes.

Discussion

Dr. DeYoung started the discussion at this meeting by admitting that his suggestion of using "\S\" or "Signed" was merely a Trojan Horse to get us to talk about and use PKI and electronically sign our FPKIPA email votes. The attendees all agreed that the FPKIPA should be using PKI technology in our business processes. The attendees also recognized that there are some implementations challenges to using PKI for FPKIPA votes, since not all of the FPKIPA voting members have established PKIs or PKIs cross-certified with the FBCA.

ACTION (094): Dr. Tice DeYoung, NASA, will research the possible options for making PKI electronic signatures a reality for FPKIPA email votes and other FPKIPA business processes.

Agenda Item 6

Discussion Topic #3: Facilitating Compliance with Annual Audit Requirements

Background

There is a FISMA requirement for all certified IT Systems to be audited annually. The FBCA CP, Section 2.7.1, repeats the FISMA requirement, as a reminder. There are no current processes in place to enforce this FISMA requirement for FBCA cross-certification members.

Discussion

The brief discussion in this meeting on this subject revolved around the fact that the FPKIPA has no mechanism or rationale for requiring annual audits, since it is a FISMA requirement. The best method, the attendees concluded, was to send a letter to the FBCA cross-certification members and ask them to send a letter to the FPKIPA to document their compliance audit history and schedule of annual audit of their cross-certified CA, in compliance with FISMA requirements.

ACTION (095): IATAC will develop, obtain FPKIPA approval, and distribute a letter to cross-certification members, requesting them to send a letter to the FPKIPA to document their compliance audit history and schedule of annual audit of their cross-certified CA, in compliance with FISMA requirements.

Agenda Item 7

Federal Identity Credentialing Committee (FICC) Report

Mr. Brant Petrick, FICC and FPKIPA webmaster, reported the following items:

The next FICC meeting will be held on 1 Dec 2004 at the E-Gov Conference in the Ronald Reagan Building.

The number of attendees at the Homeland Security Presidential Directive – 12 (HSPD-12) / FIPS 201 meetings last week were encouraging and facilitated healthy discussion about the developing standard. 125 people attended the invitation-only, Government session on 6 October and 225 people attended the Industry session on 7 October. Copies of the presentations from these sessions held on 6-7 October can be accessed at:

<http://csrc.nist.gov/piv-project>

NIST is working aggressively to meet the following schedule on HSPD-12/FIPS 201:

19 Oct 04	Target date for completion of internal draft for comments
08 Nov 04	NIST will publish first public draft of FIPS 201 standard
23 Dec 04	Comments due to NIST on first public draft of FIPS 201
18 Jan 05	FIPS 201 finished and due to the Secretary of Commerce
25 Feb 05	FIPS 201 signed by Secretary of Commerce and effective

Dr. DeYoung, NASA, stated NASA's concern that the FIPS 201 requirement of SHA-256 is too far ahead of currently available technology and policy and should be removed from FIPS 201. Mr. Polk, NIST, agrees with NASA and encourages comments about this subject be sent to NIST before 23 Dec 2004. William (Curt) Barker, NIST, is the POC for comments on FIPS 201.

Agenda Item 8

FPKI Certificate Policy Working Group (CPWG) Report

Since the 14 September FPKIPA meeting, CPWG meetings were held on 17 September and 8 October. At the 17 September CPWG meeting, the CPWG met with HEBCA representatives to discuss discrepancies in their CP, discussed comments and changes to the FBCA CP from the Asia Pacific Economic Cooperation (APEC), and had an internal-CPWG review of the GPO mapping. At the 8 October CPWG meeting, the CPWG discussed the U.S. citizenship white paper, discussed the KPMG audit letter on the Federal PKI Architecture OA (FPKIA OA), discussed some of the Wells Fargo CP General Mapping Matrix, and reviewed the GPO responses to the discrepancy letter and agreed to recommend approval to the FPKIPA of the GPO CP for the Medium assurance level.

A mapping recommendation for the Medium assurance level for the GPO CP was distributed to the FPKIPA via email prior to the meeting for review. It was unanimously approved during this FPKIPA meeting, according to the following voting record:

Approval vote for GPO CP mapping at the Medium assurance level			
Voting members	Vote (Motion – Commerce; 2nd – NASA)		
	Yes	No	Abstain
Dept of the Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Justice	X		
Dept of State (proxy by FPKIPA Co-Chair)	X		
Dept of Treasury (proxy by FPKIPA Co-Chair)	X		
GSA	X		
NASA	X		
OMB (proxy by FPKIPA Co-Chair)	X		
USDA/NFC (proxy by FPKIPA Co-Chair)	X		

The next CPWG meetings are scheduled for 2 and 23 November and 7 December.

Agenda Item 9

Federal PKI Architecture Operational Authority (FPKIA OA) Report

Status of FPKIA Certification & Accreditation (C&A)

Ms. Cheryl Jenkins, FPKIA OA Director, reviewed the status of the FPKIA Certification & Accreditation, stating the following highlights:

- The FPKIA OA currently has a Full Authority To Operate (ATO) with two residual issues, both about the “hot site”, but they are being addressed.
- KPMG is currently doing a mapping comparison of the new FBCA CP (RFC 3647) compared to the old FBCA CP (RFC 2527) to identify any requirement changes. Their findings will be documented in a report due in November.

Status of FBCA/Applicant Cross-Certification Technical Testing:

Interoperability testing with DoD External CA (DoD ECA) was completed on 1 October.

Testing with both the Patent & Trademark Office (PTO) and ACES/AT&T continues with directory testing as the last portion of testing to complete.

Status of CA Testing:

Ms. Jenkins identified an issue related to the E-Authentication PMO. Every certificate cross-certified with the FBCA is put on the E-Authentication Trust List. But since there is no working path discovery and validation solution, this is causing or will soon cause technical problems. The FPKIA OA is receiving weekly requests for test certificates from the FBCA cross-certificate members because most,

if not all of them, do not have a test infrastructure. The FPKIA OA is also receiving many questions about CAM functionality and its scalability for the future.

Agenda Item 10

Other Topics

Bridge-to-Bridge Cross-Certification

It was stated that updates to the FBCA Criteria & Methodology(C&M) document and the FPKIPA Charter need to be done to address Bridge-to-Bridge Cross-Certification.

ACTION (096): Dr. Tice DeYoung, NASA, will research and draft FPKIPA charter updates to address Bridge-to-Bridge Cross-Certification.

ACTION (097): Dr. Peter Alterman, HHS, will research and draft FBCA Criteria & Methodology document updates to address Bridge-to-Bridge Cross-Certification.

ACTION (098): IATAC will research if the FBCA Criteria & Methodology document was ever approved by the FPKIA.

Action Item Review

It was acknowledged that Action #57 and #62 are related and IATAC will work with NIST to reach closure on them.

Action #43 was declared Closed due to the redefinition of the FPKI Architecture.

Action #76 was declared Closed due to Microsoft devising a solution that didn't require the FPKIPA letter that was the subject of this original action item.

Action #90 will be rewritten to have Ms. Jenkins develop a C&A list related to NIST Standards 800-26 and 800-53.

ACTION (099): IATAC will update the Common Policy CA with Change Proposals on the FPKIPA website and forward the updated Common Policy to the FPKIPA webmaster.

Agenda Item 11

Meeting Adjourned / Next Meeting Plans

The meeting adjourned at 12:00 noon.

The next FPKI PA Meeting is scheduled for 9 November 2004 from 09:30-12:30 at the GSA facility located at 1800 F Street, Room 5141B, Washington, DC.

D. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
043	Establish policy to reflect the changing interoperability needs of the multiple membrane members, and forward requested changes to Mr. John Cornell for review before sending out to the working group members.	Tim Polk, NIST	13 May 2003	13 Jan 2004 FPKIPA meeting	Closed, 12 Oct 2004 FPKIPA meeting
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	13 Jan 2004 FPKIPA meeting	Open
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	Open
061	Incorporate the new FBCA CP Change Proposals (2003-01 through 2003-05) into the FBCA CP, dated 10 September 2002, and forward the resulting FBCA CP to the FPKIPA webmaster for posting to the Federal PKI web sites.	IATAC	9 Sept 2003	31 Dec 2003	Closed, 27 Sept 2004
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	Open
066	Develop text for the FPKIPA Charter regarding the sunset clause for voting members of the FPKIPA who are not cross certified members of the FBCA.	Tim Polk, NIST	18 Nov 2003	13 Jan 2003 FPKIPA meeting	Open
076	Check the accuracy of the dates and contact information in the Microsoft agreement (Action Item #68) and then distribute it to the FPKIPA and the CPWG.	FBCA OA	9 Mar 2004	13 Apr 2004 FPKIPA meeting	Closed, 12 Oct 2004 FPKIPA meeting
085	Test/evaluate the PKCS-12 usage issue and make a recommendation to the FPKIPA at a meeting in the near future.	Tim Polk, NIST	13 July 2004	12 October 2004 FPKIPA meeting	Open
087	Once the FPKIPA approves the Department of Labor (DoL) compliance audit letter, request the FPKIPA voting members to submit their approval votes for cross certification of DoL.	IATAC	13 July 2004	10 August 2004 FPKIPA meeting	Open

No.	Action Statement	POC	Start Date	Target Date	Status
088	Address the issue about verification of signatures from 2048 bit keys at the 14 September 2004 FPKIPA meeting	Dept of Commerce (NIST)	10 Aug 2004	14 Sept 2004 FPKIPA meeting	Closed, 14 Sept FPKIPA meeting
089	Develop an E-Governance CA CP Change Proposal for Section 2.4.2 – Dispute Resolution to make the E-Authentication PMO the mitigating authority for disputes, rather than the FPKIPA, forward it to the FPKIPA mail list for review, and request a vote.	Dept of Commerce (NIST)	10 Aug 2004	14 Sept 2004 FPKIPA meeting	Closed, 14 Sept FPKIPA meeting
090	Develop a C&A list related to NIST Standards 800-26 and 800-53.	Cheryl Jenkins, GSA	12 Oct 2004	Jan 2005 FPKIPA meeting	Open
091	Collaborate on a white paper to summarize the background, discussion points and options to address the U.S. citizenship requirement for Trusted Roles in the FBCA CP, Section 5.3.1. This will be discussed at the next CPWG meeting on 8 October 2004.	Peter Alterman, NIH; Tim Polk, NIST; and Judy Spencer, GSA	14 Sept 2004	5 Oct 2004	Closed, 1 Oct 2004
092	Send FBCA CP Change Proposal 2004-02 to the FPKIPA voting members for review and email vote during the week of 20 September 2004.	IATAC	14 Sept 2004	22 Sept 2004	Closed, 21 Sept 2004
093	Send existing definitions from any of their organizations' policy documentation or procedures/metrics for measuring "loyalty, trustworthiness, and integrity" to Dr. Peter Alterman, HHS, by 20 October 2004.	FPKIPA voting members	12 Oct 2004	20 Oct 2004	Closed, 20 Oct 2004
094	Research the possible options for making PKI electronic signatures a reality for FPKIPA email votes and other FPKIPA business processes and report back to the FPKIPA at the 9 Nov meeting.	Dr. Tice DeYoung, NASA	12 Oct 2004	9 Nov 2004 FPKIPA meeting	Open
095	Develop, obtain FPKIPA approval, and distribute a letter to cross-certification members, requesting them to send a letter to the FPKIPA to document their compliance audit history and schedule of annual audit of their cross-certified CA, in compliance with FISMA requirements.	IATAC	12 Oct 2004	14 Dec 2004 FPKIPA meeting	Open

No.	Action Statement	POC	Start Date	Target Date	Status
096	Research and draft FPKIPA charter updates to address Bridge-to-Bridge Cross-Certification.	Dr. Tice DeYoung, NASA	12 Oct 2004	Jan 2005 FPKIPA meeting	Open
097	Research and draft FBCA Criteria & Methodology document updates to address Bridge-to-Bridge Cross-Certification.	Dr. Peter Alterman, HHS	12 Oct 2004	Jan 2005 FPKIPA meeting	Open
098	Research if the FBCA Criteria & Methodology document was ever approved by the FPKIPA.	IATAC	12 Oct 2004	19 Oct 2004	Closed, 15 Oct 2004
099	Update the Common Policy CA with Change Proposals on the FPKIPA website and forward the updated Common Policy to the FPKIPA webmaster.	IATAC	12 Oct 2004	26 Oct 2004	Closed, 1 Nov 2004

Appendix A:

FPKIPA Email Voting Record (15 September–11 October 2004)

ORG	FBCA CP Change Proposal 2004-02 Requested 09/21/04 Approved 09/24/04	Voting Member	E-Gov CA CP Change Proposal 2004-02 Requested 09/21/04 Approved 09/24/04	Voting Member	Federal Common Policy Framework CA CP Requested 10/08/04 Approved 10/08/04	Voting Member
<i>Commerce</i>	Y 09/24/04	Polk	Y 09/24/04	Polk	Y 10/08/04	Polk
<i>Defense</i>	Y 09/23/04	Hanko	Y 09/23/04	Hanko	Y 10/08/04	Hanko
<i>Energy</i>	Y 09/23/04	Bales	Y 09/23/04	Bales	Y 10/08/04	Bales
<i>Justice</i>	Y 09/23/04	Burkhhouse	Y 09/23/04	Burkhhouse		
<i>State</i>	Y 09/22/04	Cao	Y 09/22/04	Cao	Y 10/08/04	Cao
<i>Treasury</i>	Y 09/23/04	Moldenhauer	Y 09/23/04	Moldenhauer	Y 10/08/04	Moldenhauer
<i>GSA</i>	Y 09/22/04	Temoshok	Y 09/22/04	Temoshok	Y 10/08/04	Temoshok
<i>NASA</i>	Y 09/22/04	DeYoung	Y 09/22/04	DeYoung	Y 10/08/04	DeYoung
<i>OMB</i>	Y 09/23/04	Thornton	Y 09/23/04	Thornton	Y 10/08/04	Thornton
<i>USDA/NFC</i>	Y 09/23/04	Sharp	Y 09/23/04	Sharp	Y 10/08/04	Sharp